

**REMARKS**

Reconsideration and allowance are respectfully requested. Claims 1-14 are currently pending, with Claims 13 and 14 being new. Claims 1-12 were rejected. Claims 10 and 12 have been amended for clarity. No new matter has been entered. Based on the following remarks, it is believed that all pending claims are in condition for allowance and a notice to that affect is respectfully requested.

I. \$112 Rejection of Claims 10-12

Claims 10-12 were rejected under 35 U.S.C. §112 as being indefinite due to use of the word "type" in the phrase "type of entitlement". In response, Claims 10 and 12 have been amended to correct the noted informality.

II. \$103(a) Rejection of Claims 1-12

Claims 1-12 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,101,477 to Hohle in view of U.S. Patent No. 5,801,367 to Asplund and U.S. Patent No. 5,953,705 to Oneda. Based on the following remarks, Applicants respectfully traverse this rejection.

A. Independent Claim 1

The current invention is a method of booking access entitlement to a facility (i.e., a weekend pass to a ski resort), where a data carrier, such as a smart card, is used to gain access to the various areas of the resort. According to Claim 1, this is accomplished by several steps, including:

determining identification data that is coded within the data carrier as well as provided visibly on the data carrier;

conveying the visible identification data, together with access entitlement data to be

booked, via a telecommunication device to the access terminal and storing it there;

(emphasis added).

B. Hohle does not disclose off-line transactions

In contrast to the claimed invention, Hohle does not disclose a method of booking access to a facility by conveying identification data and access entitlement data over a telecommunication device to an access terminal, and then upon arrival at the facility, coding the previously booked access entitlement data onto the data carrier.

Instead, Hohle discloses a travel-related smart card that must always be used in conjunction with a card issuer and one or more computer access point that connect to the Hotel. (See Figure 10) The Office Action asserts that Hohle discloses the ability to conduct off-line transactions, citing two specific passages (12:38-52 and 26:59-61) of the disclosure. However, Applicant has reviewed these passages and believes that neither supports the assertion that Hohle can conduct off-line transactions with respect to identification data and access entitlement data.

Specifically, passage 12:38-52 discloses that the smart card of Hohle can function as a user's charge card or debit card, with a payment card file section (referred to as an elementary file or EF) storing "card numbers and expiration dates for two cards". (See Hohle, 12:41-42) The passage then discloses that the charge/debit card information is stored on the smart card according to ISO-7813, an industry standard concerning a particular payment card number format. Hohle then emphasizes that this "data set is sufficient only for 'card not present' transactions, for example, transactions taking place remotely where only the card number and

expiration date are required to effect the transaction". (See Hohle, 12:47-50)

Review of the second cited passage 26:59-61 in context (i.e., also reviewing preceding lines 26:43-58) discloses that Hohle does not remotely convey identification data and access entitlement data "via a telecommunication device to the access terminal", but instead requires the smart card to be inserted into and read by the access terminal. Specifically, a cardholder can "locate a convenient access point (for example, a stand-alone kiosk in a mall) and insert the card into a provided card reader in order to initiate a transaction". (See Hohle, 26:44-46) The cardholder then interacts with the access point to conduct a transaction, where upon the access point sends the transaction data "to the appropriate partnering organization ... over a network to be stored in their respective databases. Alternatively, this data [referring to smart card data being interfaced by the access point] may be sent later as part of a card/database synchronization procedure" (See Hohle, 26:56-60). Accordingly, no visible data on the smart card is remotely conveyed via a telecommunication device to an access point. Instead, all transaction data in Hohle require the smart card to be inserted into and read by an access point. Transmission of data between the access point and a remote database then occurs in real-time via a network connection, or alternatively, the data is temporarily stored in the access point and later conveyed to the remote database as part of synchronization process. Accordingly, Hohle requires an access point before any data can be retrieved off of its smartcard and conveyed to a remote database. In contrast, the claimed invention has no such limitation as a person is able to communicate a request for a reservation using a variety of methods, such as simply calling in via a telephone and communicating the request, as well as the user's

identification data, by speech. Alternatively, one of several common data communication methods, such as short message service (SMS) over a standard mobile phone, can be utilized to make the request and relay the users identification data.

Unlike Hohle, no off-site access point/card reader is required to make a remote request in the claimed invention, a reservation can be made from any place, such as, for example, a moving car via a mobile phone.

C. Asplund does not provide identification data visibly on the data carrier

The Office Action acknowledges that Hohle does not disclose providing identification data visibly on the smart card. The reference of Asplund is subsequently cited to supplement Hohle's lack of visible data on the carrier (i.e., card). However, further review reveals that, similar to Hohle, Asplund also does not disclose the providing of identification data visibly on the data carrier.

Specifically, Asplund discloses a travel registration system that includes an electronic travel pass capable of storing various user information in addition to trip information. Incorporated into the travel pass is a LCD window capable of displaying certain specific information. (See Asplund, 3:1-10) Asplund subsequently discloses that the LCD displays "data relating to a booked journey or route". Consequently, if a check-in terminal is not functioning, the owner of the pass is still "able to show that the pass is valid because details of the journey are displayed in the display window". (See Asplund, 5:4-9) However, Asplund never discloses or suggests that the LCD can display identification data that is encoded within and identifies the data carrier (i.e., card).

D. Asplund requires the storage of additional data that can lead to a significantly larger database

The method for booking access entitlement to a facility, as called for in Claim 1, only requires the encoding of identification data (i.e., a serial number that uniquely identifies the carrier, not the person in control of the carrier) and access entitlement data (i.e., 2 day ski pass) onto the data carrier. This allows for a more minimal and efficient databases, as well as smaller memory requirements for both the carrier and the access terminal. Another consequence of relying on identification data encoded onto and identifying the carrier (i.e., card) and not user-specific data is that use of the carrier is not restricted to one person.

In contrast, Asplund discloses the storing of numerous pieces of information, including various user information (i.e., name, address and telephone number), onto its travel pass and associated databases. (See Asplund, 4:7-21) This can lead to larger and less efficient databases, as well as increased memory requirements. In addition, use of the travel pass is restricted to one person. Indeed, Asplund discloses the incorporation of a biometric scanner (i.e., fingerprint scanner) into its travel pass, thereby allowing a user of the pass to verify that they are the same user as identified by the user information stored upon the pass. (See Asplund, 3:50-4:6, 4:54-5:3)

E. Oneda does not disclose off-line transactions

The reference of Oneda is further cited as a supplement to the disclosure of Hohle. However, a detailed review of Oneda reveals that, similar to Hohle, Oneda does not disclose the ability to conduct off-line transactions.

Specifically, Oneda discloses a ticketless system for processing and issuing airplane tickets. A user acquires an

IC card, which then has to be registered with a reservation system that maintains a database comprised of various information files, including a purchase information, career information, customer information, coupon ticket information and discount rate information. (See Oneda, 8:25-33) A user purchases one or more flight credits or coupons that can be exchanged for tickets. The user subsequently takes their IC card (now referred to as a distribution source card) and inserts it into a ticket issuing machine, where they can carry out various functions such as boarding reservations, ticket issue, check-in, seat assignments, etc. In addition, the user can transfer part or all of their flight coupons to another user account registered in the reservation system. (See Oneda, 7:2-16) However, as indicated by every example in the disclosure, Oneda always requires a user's IC card to be inserted into either a "counter terminal apparatus" or "automatic ticket issuing machine", both of which are in communication with the system's master database, before data can be read from the card and used to conduct transactions. Accordingly, unlike the method called for in Claim 1, Oneda does not disclose the "conveying of "visible identification data ... [and] access entitlement data ... via a telecommunication device to the access terminal".

F. Oneda requires the storage of additional data that can lead to a significantly larger database

Similar to Asplund, the system disclosed in Oneda stores within its system numerous information beyond the identification data of a card and access entitlement data. Some examples include a use range such as an interval or the like, the number of times a coupon has been distributed, and the number of times the IC card has been used, as well as individual information such as user ID, age, purchase date and location, etc. (See Oneda, 2:40-65)

G. Combination of the cited references is illogical  
and would destroy their intended purpose

The Office Action asserts that the method of Claim 1 is unpatentable over a combination of Hohle with Asplund and/or Oneda. Specifically, it is asserted that it would have been obvious to have included in Hohle the visible data of Asplund in order to allow the user to ascertain the card ID without using a card reader. If the visible ID information is printed on the card rather than electronically displayed, then such would have been obvious in view of Oneda.

However, as discussed above, the prior art of Asplund only discloses the display of trip information, not a card ID. One could presume, for argument's sake, that the displayed identification data disclosed in Oneda could be incorporated into Hohle or Asplund. However, further inspection reveals that due to the different nature and purpose of all three prior art systems compared to Claim 1, the addition of a visual indication of a card's encoded identification code would destroy the intended purpose of the prior art systems as such a modification would weaken their security.

Consider Claim 1, which calls for a method of booking access entitlement to a facility such as a ski resort. Relatively speaking, such a task requires little security. The data carrier is identified by the encoded identification code, such as card serial number, which is read by the access terminal. No encoding of data concerning the identity of the user is required.

In contrast, all three prior art references disclose ticket systems that are utilized in the airline industry, an environment that requires a heightened level of security. The identity of the user, as well as the security of the system and its data, becomes paramount. To that end, knowledge of the encoded ID of a smartcard becomes a very sensitive piece

of information in terms of system security, especially when combined with knowledge of the user identity associated with that smartcard. In that respect, providing a visual indicator of a card's encoded ID could lead to increased risks unless otherwise compensated by additional security features.

For instance, the reservation system of Oneda, which for argument's sake is presumed to display a card ID, also incorporates a key pad into the card upon which a user must enter a personal identification code before the card can be used. In contrast, the system of Hohle, which discloses no additional security features such as that of Oneda, would suffer a decrease in security if the system were modified to include a visual depiction of the card ID. Accordingly, once you consider the underlying purpose of the prior art systems, it becomes apparent that instead of motivation to combine the prior art, there is actually motivation to not combine the prior art systems.

#### H. Independent Claim 10

Independent Claim 10, as amended, calls for a method for remotely booking access entitlement to a facility using a portable data carrier that is encoded with identification data as well as visibly marked with the identification data, comprising the steps of:

establishing a remote communication link with a computer server associated with the facility;

manually providing the identification data over the remote communication link to the computer server of the facility;

selecting a desired access entitlement and conveying the selection over the remote communication link to the computer server of the facility;



storing the provided identification data and selected access entitlement on the computer server;

identifying a user upon arrival at the facility by electronically reading the identification data encoded on the data carrier using an access terminal that communicates with the computer server; and

retrieving the previously selected access entitlement associated with the provided identification data and stored in the computer server, and forwarding the selected access entitlement onto the access terminal; and

encoding the associated access entitlement onto the data carrier using the access terminal;

wherein any further authorization at the facility for the selected access entitlement is obtained by electronically reading the identification data and associated access entitlement encoded on the data carrier

(emphasis added).

However, as previously discussed, the prior art of Hohle does not disclose visibly providing identification data on the data carrier. Additionally, Hohle fails to disclose "establishing a remote communication link with a computer server" and "manually providing the identification data over the remote communication link to the computer server".

Similarly, Asplund neither discloses nor suggest visually providing identification data on the data carrier, as well as requiring the storage of additional data such as user information.

The reference of Oneda is also found to neither disclose nor suggest an ability to do off-line transactions, such as by "establishing a remote communication link with a computer server". In a manner similar to Asplund, the reference of Oneda also requires the storage of additional data, such as user information.

Lastly, as discussed in detail above, there is no motivation to combine the references as it would be illogical and would negatively impact their intended purpose.

For the above reasons, Applicant believes that Claims 1-12 are allowable over the references of Hohle, Asplund and Oneda, considered either individually or in combination.

### III. Claims 7 and 8

Dependent Claims 7 and 8 were never addressed in the Office Action, and as such, it is not clear whether these claims are in an allowable condition or were intended to be rejected on the basis of the §103(a) rejection discussed above. Regardless, Applicant believes that dependent Claims 7 and 8 are allowable over the cited references for the same reasons as discussed above with respect to the other claims.

### IV. New Claims 13 and 14

New independent Claim 13 calls for a method for remotely booking access entitlement to a facility, comprising, among other things, the steps of:

providing a smart card containing a passive RFID transponder; and

providing an identifier code that is unique to the smart card and which is visibly presented upon the smart card as well as encoded on the passive RFID transponder within the smart card

(emphasis added).

Applicant believes that Claim 13 is allowable over the cited prior art for reasons similar to those previously discussed with respect to Claims 1 and 10.

In addition, the requirement of a passive RFID transponder further distinguishes Claim 13 from the prior art of Asplund. Specifically, Asplund discloses a travel pass unit or smart card that includes a processor and LCD display

that are actively powered by a power pack incorporated into the card. (See Asplund, 3:30-50) In contrast, Claim 13 calls for a passive RFID transponder, which by definition, does not contain its own power source but is instead powered by an access terminal through electromagnetic induction.

For the above reasons, Applicant believes that independent Claim 13 and dependent Claim 14 are allowable over the cited prior art, considered either individually or in combination.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance, and a Notice to that effect is earnestly solicited.

Respectfully submitted,

  
Steven R. Thiel

SRT/cc

FLYNN, THIEL, BOUTELL  
& TANIS, P.C.  
2026 Rambling Road  
Kalamazoo, MI 49008-1631  
Phone: (269) 381-1156  
< Fax: (269) 381-5465

Dale H. Thiel	Reg. No. 24	323
David G. Boutell	Reg. No. 25	072
Ronald J. Tanis	Reg. No. 22	724
Terryence F. Chapman	Reg. No. 32	549
Mark L. Maki	Reg. No. 36	589
Liane L. Churney	Reg. No. 40	694
Brian R. Tumm	Reg. No. 36	328
Steven R. Thiel	Reg. No. 53	685
Donald J. Wallace	Reg. No. 43	977
Kevin L. Pontius	Reg. No. 37	512
Sidney B. Williams, Jr.	Reg. No. 24	949

Encl: None

136.07/05